



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/068,294	02/05/2002	George Robert Blakley	LYRN002US0	9653
58293	7590	10/16/2006	EXAMINER	
FORTKORT & HOUSTON P.C. 9442 N. CAPITAL OF TEXAS HIGHWAY ARBORETUM PLAZA ONE, SUITE 500 AUSTIN, TX 78759			PYZOCHA, MICHAEL J	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 10/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 10/068,294	Applicant(s) BLAKLEY ET AL.	
	Examiner Michael Pyzocha	Art Unit 2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 19 September 2006.
- 2a) ☒ This action is FINAL. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 32-59 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 32-34, 36-47, 49, 50 and 52-59 is/are rejected.
- 7) ☒ Claim(s) 35, 48 and 51 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date <u>20060919</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 32-59 are pending.
2. Amendment filed 09/19/2006 has been received and considered.

Claim Rejections - 35 USC § 112

3. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

4. Claims 52-59 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.
5. Claim 52 rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: how the modulus C in claim 32 is tied to the calculations performed in claim 52. It appears the steps being performed in claim 52 more closely relate to the steps being performed in claim 33 as opposed to claim 32.
6. Any claim not specifically addressed is rejected by virtue of its dependency.

Art Unit: 2137

Claim Rejections - 35 USC § 102

7. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless -

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

8. Claims 32, 34, 36-46, 49, and 50 are rejected under 35 U.S.C. 102(b) as being anticipated by Silverman et al. ("Recent Results on Signature Forgery").

As per claims 32, 38 and 39, Silverman et al. discloses a method for encrypting data comprising choosing a modulus C for modular calculations, wherein C is a w-bit number, and wherein the modulus C is selected from the group consisting of (a) w-big and w-heavy, and (b) w-little and w-light; and using the modulus to encrypt data (see section 3 pages 3-4).

As per claims 34 and 40-46, Silverman et al. discloses receiving data; and using a modulus C to encrypt the data, wherein C is a w-bit number, wherein the modulus C is of the form $2^w - x$, wherein $x = \pm L$, wherein L is a low Hamming weight odd integer less than $2^{(w-1)/2}$ and wherein the modulus C is selected from the group consisting of (a) w-big and w-heavy, and

Art Unit: 2137

(b) w-little and w-light; and outputting the encrypted data (see section 3 pages 3-4).

As per claims 36 and 49, Silverman et al. discloses the modulus C in the form $2^w + L$ has a Hamming weight close to 1 (see section 3 pages 3-4).

As per claims 37 and 50, Silverman et al. disclose the encrypting of data comprises cryptographic hashing (see section 3 pages 3-4).

Claim Rejections - 35 USC § 103

9. Claims 33 and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Silverman et al. as applied to claims 32 and 40 above, and further in view of Menezes et al. (Handbook of Applied Cryptography).

As per claims 33 and 47, Silverman et al. fails to disclose performing a ring arithmetic function on numbers, including (a) using a residue number multiplication process, (b) convening to a first basis using a mixed radix system, and (c) converting to a second basis using a mixed radix system.

However, Menezes et al. teaches the use of such conversion (see pages 611-612).

Art Unit: 2137

At the time of the invention it would have been obvious to a person of ordinary skill in the art to perform the mixed radix system in the Silverman et al. system.

Motivation to do so would have been that the computations are faster (see Menezes et al pages 611-612).

Allowable Subject Matter

10. Claims 35, 48 and 51 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

11. Claims 52-59 would be allowable if rewritten to overcome the rejection(s) under 35 U.S.C. 112, 2nd paragraph, set forth in this Office action and to include all of the limitations of the base claim and any intervening claims.

12. The following is a statement of reasons for the indication of allowable subject matter: The prior art teaches the use of specific modulus C values but does not teach the specific calculation of modulus C as described in claims 35 and 48, specifically two steps of splitting. Nor does the prior art teach or reasonably suggest the value C taking the specific form put forth in claim 51. The prior art also does not teach or

Art Unit: 2137

reasonably suggest the method of calculating performed in claim 52.

Response to Arguments

13. Applicant's arguments filed 09/19/2006 have been fully considered but they are not persuasive. Applicant argues Silverman does not teach any of: w-big, w-heavy, w-little or w-light numbers; Applicant alleges Examiner relied upon inherency; the Silverman reference teaches away from a combination with Menezes.

With respect to Applicant's argument that Silverman does not teach any of: w-big, w-heavy, w-little or w-light numbers, it is clear that Silverman teaches w-big and w-little numbers because Silverman teaches that the modulus takes the form $2^k \pm c$ where c is small. Therefore when c is small and we take the subtraction case the modulus is less than 2^k but close to 2^k , which is clearly defined as a w-big number. Similarly, when c is small and we take the addition case the modulus is greater than 2^k but close to 2^k , which is clearly defined as a w-little number. As w-big and w-little are defined on page 20 of the specification. Furthermore, to show that $2^k \pm c$ where c is small is also w-heavy and w-light it must be known that 2^k takes the form 10...0 in binary for all k that are positive integers where

Art Unit: 2137

the "0...0" contains k zeros. Therefore when we take a small value of c , say one, it is clear by basic binary arithmetic that $2^k - 1$ will take the form of 1...1 where there are k ones which has a hamming weight of exactly k which is clearly close to k the and $2^k - 1$ is less than but close to 2^k therefore a w-heavy number as defined by the specification. Similarly, when we take a small value of c , say one, it is clear by basic binary arithmetic that 2^{k+1} will take the form of 10...01 where there are $k-1$ zeros which has a hamming weight of two which is close to one and 2^{k+1} is greater than but close to 2^k therefore a w-light number as defined by the specification.

With respect to Applicant's allegation that Examiner relied upon inherency Examiner nowhere relied upon inherency for anticipation of Applicant's claims. Furthermore, as put forth above, the Silverman reference clearly discloses w-big, w-heavy, w-little and w-light numbers.

With respect to Applicant's argument that Silverman teaches away from a combination with Menezes, Silverman teaches that only specific values of the modulus should be avoided, not that the whole standard should be avoided. Therefore Silverman does not teach away from the combination and one of ordinary skill in the art would still be motivated to perform the calculations

Art Unit: 2137

taught by Menezes in the standard taught by Silverman to speed up the calculations.

Conclusion

14. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

Art Unit: 2137

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

MJP


EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER